CLEARING INFORMATION FROM YOUR COMPUTER'S HARD DRIVE

Office of Inspector General

National Aeronautics and
Space Administration

An Information Technology Security Alert

THE THREAT

You have probably heard accounts of hackers who break into computer systems on the Internet to steal secrets or other sensitive information, and others who hack just for the challenge of penetrating system security. However, there is another way that people can get access to sensitive information on your computers—by simply reading it from the hard drives after the computers have left your control. The theft of this data can defeat data security within your Agency, and also compromise the privacy of the user. Here is what you should know:

DATA STORAGE

Technological advances in computer hardware and software have resulted in employee workstations being upgraded and replaced on a frequent basis. Information stored on the old computer is copied onto the hard drive of the new system and the employee's work continues. However, what happens to the old computer and its hard drive? Did it leave with any sensitive information or information protected by the Privacy Act stored on it? Replaced computers are not destroyed, but usually are transferred to other Federal users, contractor users, donated to educational institutions, or sold to the public for reuse.

In performing daily work assignments, most of us make extensive use of personal computer capabilities. All personal computers, whether at home or at work, contain internal storage devices called hard drives.

Each assignment that we undertake generates new electronic files and folders for collecting volumes of data, memos, reports, data spreadsheets, correspondence, and e-mails. Over time, data files are saved to and deleted from this storage media. Where hard copy, paper documents once were kept in folders stored in office filing cabinets, now electronic documents are stored in electronic folders created on the computer's hard drive—a tremendous space saving development, but a much less visible medium. From time to time, we delete documents to free up space on our hard drives or because the files are outdated and considered unnecessary. However, hitting the "delete" key is not the end of the story. Do you believe that when you delete a file that it is completely gone? It may surprise you to know it is not—and this poses a real information security threat.

TECHNICALLY SPEAKING

As an example, one personal computer operating system lists the file names and information about a file's location on a computer hard drive in a master index called the File Allocation Table (FAT). When you execute a command to delete or erase a file from your computer's storage (using your "delete" key or mouse), the FAT is modified so that it no longer shows the file as being on the disk. This is comparable to removing a chapter listing in a book's table of contents. By removing this reference, the computer's operating system is telling the computer that this storage location is now available to receive any newly saved data. But until a new file actually writes over a file storage location, the file that you deleted is still on the hard drive. What is frightening about this is that by using software known as a low-level disk editor (freeware, or often commercially available for less that $40), anyone with elementary computer skills can retrieve the information.

NOW YOU SEE IT...
NOW YOU DON'T...
NOW YOU DO...

In an attempt to clean the hard drive of all stored information, technicians sometimes repartition and reformat the drive using standard operating system commands. However, this only redefines the drive's internal characteristics to prepare it to store future information. The FAT index is cleared of all entries and a directory listing will display that the hard drive appears file free. This gives the illusion that the hard drive is free of stored information when the files are physically still embedded on the drive's storage media. A low-level utility program can still retrieve this data easily.

THINK ABOUT IT

By now you should be thinking about all of the computers your office previously excessed, sent out for repair, or provided to someone else, and all the files you thought you erased or deleted. How about the computers your office transferred to other users down the hall or even to another Federal agency? Imagine what a utility program in the wrong hands could extract from those drives! What kinds of information do you think might be embedded on a desktop computer removed from offices located in Payroll, Personnel, General Counsel, Procurement, or Security?

Think further. What about your home computer? Do you ever take office work home with you and create or copy files onto that computer's hard drive? Remember that old, first generation computer you owned and donated to goodwill or the Salvation Army? Or the one you sold for one-tenth of what you paid for it? Does it have your personal financial information on it that you thought you deleted? Is there any social security, driver's license, date of birth, phone directory, or medical information residing on it that you thought you had deleted? Do you not consider this information to be sensitive and not to be shared with others indiscriminately?

WHAT CAN BE DONE?

Many popular utility programs are available commercially to ensure that data is unrecoverable when you erase files. These utilities actually overwrite the entire hard disk with a pattern of characters, rendering the previous information unrecoverable. Executed properly, every character position is overwritten throughout the entire drive, clearing it of user data imprinted at all levels.

Within the Federal government, your computer services support staff should be able to assist you in identifying the appropriate software to effectively clear data from your computer's hard drive. However, we have found through spot check inspections that, unfortunately, some technical support units have not always been successful in removing data from hard drives being transferred or excessed. In NASA, the Chief Information Officer (CIO) and

Center-level CIO representatives have specific policies, referenced in NPG 2810, Section 4.1.13, Security of Information Technology. We encourage you to review this policy on this Web site: *http://www.hq.nasa.gov/office/codea/codeao/xnotice.html.* Check with your local CIO office for specific details on how to ensure that your computer's hard drive is effectively cleared of data before it leaves your area of control. (Note: It is very important to remember that computers that process secret or classified files are subject to much more stringent sanitation methods. Confer with your office's designated security officer for guidance in cleansing these computers.)

Information security is not an issue limited to your work; it also presents a personal privacy threat for you at home. If you use your computer at home for work purposes, files on this computer are just as vulnerable to being recovered as those on your office computer. Your office support staff should be able to instruct you on how to run government-furnished software to cleanse your drive effectively when you decide to throw away, sell, or donate your home computer. Remember, too, that your home computer also may contain your own personal, private information embedded on the drive—even if you think you have erased or deleted those files.

ARE COMPUTER HARD DRIVES YOUR ONLY CONCERN?

Computer hard drives are the most prevalent source of stored information, but several other electronic media could also contain potentially sensitive information in memory storage. Examples include floppy discs, zip discs, CD high-end printers (laser and impact), some facsimile (fax) machines, telephone answering machines (recording type), voice messaging-paging systems, and many more. You should exercise caution when disposing of these devices—if in doubt, seek authoritative advice.

In the years to come, there will be more and more users of even more sophisticated information technology devices. With these advances will come new vulnerabilities with which you should be concern—not only for the information security of the government, but also to protect your own personal privacy.

National Aeronautics and Space Administration

AN INFORMATION TECHNOLOGY SECURITY ALERT

HOTLINE

1-800-424-9183

Toll Free 24-Hour Answering Service

or write to

NASA Office of Inspector General
P.O. Box 23089
L'Enfant Plaza Station

INFORMATION IS CONFIDENTIAL

Caller May Remain Anonymous
Report: Fraud, Waste, Abuse